INDEPENDENT COMMUNITY BANKERS of AMERICA

9

October 14, 2003

Public Information Room
Office of the Comptroller of the Currency
205 E Street, SW
Mail Stop 1-5
Washington, DC 20219
Attention: Docket No. 03-18

Ms. Jennifer J. Johnson, *Secretary*
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue, NW
Washington, DC 20551
Re: Docket No. OP-1155

Robert E. Feldman, *Executive Secretary*
Attention: Comment/OES
Federal Deposit Insurance Corporation
550 17th Street, NW
Washington, DC 20429

Regulation Comments
Chief Counsel's Office
Office of Thrift Supervision
1700 G Street, NW
Washington, DC 20552
Attention: No. 03-35

Re: **Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice**

Dear Sir or Madam:

The Independent Community Bankers of America (ICBA)[1] appreciates the opportunity to comment on the guidelines that the federal banking agencies have proposed for responding to instances of unauthorized access of customer information. In part, the guidelines are designed to provide tools for bank customers to address instances of potential identity theft.

The ICBA agrees with the agencies that identity theft is a serious problem. For example, a recent FTC survey found that last year identity theft losses to businesses and financial institutions, including existing credit card account and checking account fraud, totaled nearly $48 billion. However, because identity theft takes so many forms from simple fraud to outright usurpation of identity, and because the nature of the fraud is constantly evolving, the ICBA does not believe that a proscriptive, detailed response requirement such as that being proposed by the agencies is the best approach to unauthorized access of customer information. Instead, the ICBA recommends that the agencies offer a set of "best practices" that allows individual banks the ability to assess each unique situation and respond in the most appropriate way for those specific circumstances.

[1] ICBA is the nation's leading voice for community banks and the only national trade association dedicated exclusively to protecting the interests of the community banking industry. ICBA has nearly 4,600 members with branches in more than 17,000 locations nationwide. Our members hold more than $526 billion in insured deposits, $728 billion in assets and more than $405 billion in loans for consumers, small businesses, and farms. They employ more than 231,000 people in the communities they serve.

BACKGROUND

Before implementing new regulatory guidelines as requirements to address identity theft, it is important for the agencies to recognize that other steps are in place or being taken that address instances of unauthorized access to customer information. Perhaps most significantly, Congress is very likely to adopt revisions to the Fair Credit Reporting Act that includes important provisions designed to deter identity theft.

All banks must already have in place procedures for safeguarding customer information, as required by the *Interagency Guidelines Establishing Standards for Safeguarding Customer Information.*[2] The *Interagency Guidelines* require banks to identify reasonably foreseeable threats that could lead to unauthorized access of customer information and take appropriate steps to control the potential risk. Furthermore, the guidelines provide that bank policies and procedures to protect customer information should be tailored to the bank's size and scope of activities. A bank's security program should also take into account service providers, and contracts with service providers should require the vendor to notify the bank if there are any security breaches involving customer information.

Beyond complying with the mandates of the *Interagency Guidelines,* ICBA members have taken steps to notify customers about the dangers of identity theft and how to take appropriate steps to guard against it. Although an informal survey of ICBA leadership bankers suggests that few instances of identity theft have impacted their customers' bank accounts, community bankers, along with the rest of the industry, are taking a proactive approach to deter identity theft. The same survey of ICBA leadership bankers shows that banks are distributing brochures on identity theft,[3] providing warning messages on account statements or providing information through statement stuffers. ICBA members have also designated special employees to serve as counselors to address instances of identity theft.

THE AGENCIES' PROPOSED ADDITION TO THE GUIDELINES

The current proposal is designed to build on the existing *Interagency Guidelines* by requiring all banks to develop a response program, including procedures for providing timely notice to customers, when incidents of unauthorized access to customer information could result in substantial harm or inconvenience to the customer.

The proposal would establish very specific requirements for banks to take as a response whenever there is or may have been an instance of unauthorized access to customer information. Generally, the proposal would require a response program to include the following elements:

- Assess the situation to determine the nature and scope of the incident
- Notify the bank's primary federal regulator and, where warranted, file a Suspicious Activity Report (SAR)

---

[2] The guidelines were issued under requirements of the Gramm-Leach-Bliley Act.

[3] The ICBA offers members a brochure for distribution to customers entitled *Protect Your Good Name: Protecting Yourself from Identity Theft.* The brochure offers guidance for community bank customers on how to protect against identity theft and steps to take if it occurs. Information about the brochure is available at www.icba.org.

- Implement steps to contain and control the incident, such as shutting down applications or third party connections, reconfiguring firewalls, ensuring that all known vulnerabilities have been addressed, changing computer access codes, modifying physical access controls and placing additional controls on service provider arrangements
- Adopt measures to protect affected customers once the situation has been assessed and controlled, including providing notice to customers

Protecting Customers. The proposal specifies steps banks should take to ensure that affected customers are protected. The proposed guidelines state that the bank should have procedures in place to flag and secure accounts and provide notice and assistance to customers that may have been affected by unauthorized access to sensitive customer information. If a bank were unable to identify which customers may have been affected, the guidelines would require notice to all groups of customers that may have been affected.[4]

According to the proposal, notice to customers should be timely, clear, and conspicuous, but banks should not forgo notifying customers merely to avoid embarrassment or inconvenience. The proposal also sets out a number of very specific details for the form and contents of the notice to customers, such as a general description of the incident and information to customers to help them mitigate potential harm, including a customer service number at the bank that customers can call.

Finally, the guidelines offer examples of instances that require customer notice and those that do not. For example, notice would be required if an employee has obtained unauthorized access or if a cyber intruder has broken into the bank's databases, but would not be required if the bank determines that information improperly discarded was destroyed before any harm occurred or a hacker accessed only customer names and addresses.

GENERAL COMMENTS

Regulatory Burden. The ICBA believes that instead of implementing prescriptive, unnecessarily burdensome guidelines that lack the necessary flexibility to address unique problems in a particular situation, the agencies should inform banks of best practices that individual banks could use for reference and adapt appropriately. The proposal provides the basis for a set of best practices, but any best practices should also incorporate risk-based elements and allow banks to use discretion in their response measures. The greater flexibility offered by best practices would help banks respond and adapt their responses to changing circumstances in an extremely dynamic environment, avoid unnecessary notice to customers that may cause undue alarm, and avoid unnecessary costs and burdens for the industry.

The ICBA is concerned that implementation of the guidelines in their current format will be unduly burdensome for all banks, but especially small community banks that do not have the human, financial or other resources of larger banks. Compliance with the proposal would require banks to devise and adopt written policies that may or may not cover every instance of unauthorized access. As a result, such policies would need constant updating as hackers and other perpetrators of fraud devise new schemes. At the outset, the most

[4] The proposed requirement would parallel recently enacted California law requiring California banks to notify customers if their information may have been subjected to unauthorized access.

burdensome elements of the guidelines would be creating a general policy, establishing procedures and training staff. Developing and implementing new procedures for determining when, where and how to provide notice and procedures for monitoring accounts will also be burdensome.

The agencies should also recognize that costs would be passed along to bank customers, and the benefit to the customer against the potential risk should be factored into the equation. It is somewhat ironic that the agencies would propose potentially burdensome guidelines with no clear demonstration of need at the same time the agencies are engaged in a process of reviewing all regulations for regulatory burden under Congressional mandate.[5]

Undesirable Impact on Customers. Another concern is the undue stress that unnecessary notification may cause bank customers and the possible damage to customer relationships. If adopted as proposed, banks and thrifts will be more likely to resolve any doubts about providing notification by notifying customers, including notice for relatively minor breaches of customer information systems. As customers receive these notices from a variety of financial institutions, they will become hardened to their impact and begin to ignore them as they ignore so many other disclosures that are provided under federal regulation and notification will not have the intended effect, despite the cost and burden of production. Moreover, notice for relatively minor breaches may cause customers undue alarm.

Flexibility Needed. As proposed, the guidelines establish a one-size-fits-all approach. The ICBA strongly believes that it would be preferable to allow flexibility to take into account a bank's size, operations and risk profile. It is true that where there is a breach, all customers affected should be treated alike. It is also true that the size of the bank does not change the likelihood that it will be targeted for unauthorized access to customer information. However, smaller banks often have closer relationships with their customers and are more likely to detect suspicious activity quickly, such as when a long-standing reliable customer has an account that is suddenly overdrawn or submits a request for an inappropriate address change. Mandating specific solutions could require capital-intensive solutions, but best practices would allow each bank to assess the risk presented by the particular circumstances, determine whether the bank's response sufficiently controls the situation, notify customers *only as appropriate*, and include only pertinent information in any notice provided on a case-by-case basis.

ICBA COMMENTS ON SPECIFIC ELEMENTS OF THE PROPOSAL

Notice to Regulators. The guidelines would require banks to notify their primary federal regulator of instances of unauthorized access to customer information. While it may be appropriate to notify regulatory authorities when there has been a significant breach that may affect many customers or result in substantial costs, the proposed requirement is too broad since it requires notice whenever there has been unauthorized access that *could* result in substantial harm or inconvenience. Notice to regulators should be limited to situations where it is clearly merited and not for minor instances, especially if the bank is able to institute controls

[5] The Economic Growth and Regulatory Paperwork Reduction Act of 1996 (EGRPRA) requires the agencies to review all regulations and eliminate or recommend legislative changes to eliminate or revise regulations that are outdated, unnecessary or unduly burdensome. The importance of this effort is demonstrated by the agencies' independent website on the project at www.egrpra.gov.

that address the situation and there is no serious risk to customers or the bank as a result of the breach.

Where notice is merited, the ICBA recommends that the agencies provide contact information so it is clear exactly where the notice should be filed.

Definition of Sensitive Customer Information. The guidelines would require banks to provide notice to customers whenever "sensitive customer information" may have been breached. "Sensitive customer information" would be defined as a customer's social security number, personal identification number (PIN), password, or account number in conjunction with a personal identifier, such as the individual's name, address, or telephone number. It would also include any combination of components of customer information that would allow someone to log onto or access another person's account, such as user name and password.

The ICBA believes this definition is appropriate, since it helps limit instances when notice is required to situations that could result in access of a customer's account or possible identity theft. However, rather than requiring notice when sensitive customer information *may* have been breached, notice should only be required when sensitive customer information *has* been breached.

Standard for Providing Notice to Customers. Under the proposed guidelines, a bank would not be required to notify customers if unauthorized access to sensitive customer information occurs as long as the bank can reasonably determine that the breach would not be likely to result in the misuse of the information. The ICBA believes it is especially important to allow banks this flexibility since it allows each bank to assess the situation and act as appropriate, since the bank is in the best position to determine the level of threat to the security of customer information. If a bank determines that the breach presents sufficient risk, it can notify customers.

Allowing banks this flexibility is also important because it allows the bank to assess the risk against unnecessarily alarming customers or placing undue stress on customer relationships. It is also important to recognize that notice may do more harm than good in some circumstances. For example, if a fraud is sufficiently egregious, law enforcement may become involved but not want notice sent, since widespread notice might also alert those perpetrating the fraud. The ICBA recommends that the proposal be refined to reflect these concerns.

As noted, the ICBA believes that best practices are far preferable than prescriptive requirements. While as a theoretical standard, the proposed guidelines for when to provide notice may be appropriate, how successfully they can be applied as a practical matter depends upon interpretation by regulatory agencies, individual examiners and banks and thrifts. For example, the proposal seems to suggest that the mere occurrence of unauthorized access implies that the compromised information will be misused. Certainly, this is an interpretation that could be applied by examiners, especially since some examiners have a tendency to read any recommendation as mandated. If so construed, the bank would be in the impossible position of having to prove a negative proposition to avoid issuing notices, even where there is no evidence of actual misuse of the information.

Therefore, if the agencies decide to implement guidelines, additional guidance will be needed for what constitutes an "appropriate investigation" that would allow a bank to "reasonably conclude that misuse of the information is unlikely to occur." It should also be clarified that compliance with an example creates the presumption that the bank has acted appropriately.

Timing of Notice. The proposal would provide that a bank should furnish notice to affected customers "whenever it becomes aware of unauthorized access to sensitive customer information." The ICBA recommends that greater flexibility be incorporated into this standard. For example, as noted above, there may be situations where law enforcement or regulators become involved and want to investigate before notice is sent to customers, a step that would not likely be possible given the extremely brief timeframes in the proposal. Moreover, banks should be allowed to delay notice until sufficient information about the occurrence can be collected through research and investigation to provide customers with appropriate information to allow them to take the necessary steps to guard against identity theft and other misuse of their information.

Elements of Customer Notice. The proposal would establish specific elements to be included in a customer notice: a customer service number for customers to call; a reminder that customers should be vigilant over their accounts for the next 12 to 24 months; a statement that the bank will help correct and update credit reports; a recommendation that the customer notify the national credit reporting agencies to place a fraud alert; a recommendation that the customer periodically obtain copies of his or her credit report from each credit reporting agency; information on how to obtain a free credit report if the customer believes the report contains inaccurate information due to fraud; information about the FTC's online guidance regarding steps to take to protect against identity theft (including the FTC's Web site address and toll-free number).

While the ICBA believes that these may be appropriate elements for notice, each bank should be able to determine which items to include when notifying customers. For example, if issuing a new account number would address the problem and eliminate further risk to the customer, additional information required in the proposal may be superfluous. Similarly, the reminder that a customer should remain vigilant over the ensuing several months may not be appropriate; if unauthorized access were limited to products or services that could be secured through closure, change of password or other means, or the security breach did not result in disclosure of customer information that could readily be used to commit other forms of identity theft, there would be no need for the customer to monitor the activity on compromised but closed accounts. And, when notice is provided, it should be limited to situations of actual breach, providing customers pertinent information for monitoring account activity or taking other steps appropriate for that situation.

Banks have access to general information brochures on identity theft that cover much of the information the proposal would require, such as notification to the national credit reporting agencies. Rather than recreating this in a separate notice, enclosing a copy of such a brochure should be deemed sufficient.

If the agencies decide to maintain the requirement for an extensive notice, then the ICBA recommends the agencies develop a model notice that incorporates all the mandated elements yet allows banks to incorporate additional information where appropriate.

Securing Accounts. The proposal would require the bank to "secure accounts" following a breach of customer information. However, the guidelines do not explain what is meant by "secure accounts," although the proposal does set forth additional steps for the bank to take, such as flagging affected accounts and taking other steps to contain and control the incident. If steps such as flagging and monitoring accounts are elements of securing accounts, then that should be clarified. Otherwise, further definition is needed for what is required to "secure accounts."

The ICBA recommends that a set of best practices include a checklist for banks to use when instances of breaches are detected. Best practices could include suggestions for how long a bank should monitor accounts, with the term for monitoring commensurate with the type of breach and the potential threat of abuse of customer information to avoid needless monitoring of accounts for a long period of time.

Flagging and Monitoring Accounts. Not all bank software systems are capable of flagging and monitoring accounts. Instead, the monitoring must be done manually. Many systems do allow flags to be placed on customer records to generate reports or place flagged records into specified processing queues, but do not have the separate capability of monitoring accounts, which must be done daily on a manual basis. Until automated solutions are available for monitoring, this will be burdensome and time-consuming process. Even if software solutions are developed, it is likely that they will be expensive and potentially beyond the reach of smaller banks, meaning smaller institutions will still have to rely on manual processes.

The level of burden will depend on factors such as the frequency of review required, the number of parameters required to identify the affected activity, the number of products and services to be monitored for each individual customer, and the extent to which activity on an account triggers additional transactions. For a large breach, this requirement could be very burdensome. Therefore, rather than mandating a specific step such as monitoring affected accounts, the ICBA believes each bank should be allowed to resolve the problem in an appropriate manner, especially if the bank determines there is minimal or no risk to customers.

Vendor Contracts. Currently, not all vendor contracts include provisions that require the vendor or service provider to notify the bank if there has been a breach of customer information data. Banks, especially community banks, do not always have the bargaining power to allow them to demand such provisions in vendor contracts. Therefore, if this provision becomes effective, it will be critical to grandfather existing contracts and allow a transition period. Second, intervention by the agencies with vendors and software providers may be needed to ensure that these provisions are included.[6]

Examples. The proposal includes a variety of examples of when customer notice would and would not be necessary. The ICBA believes that providing examples is helpful, since it offers additional guidance for banks and examiners for determining the appropriate course of action and helps clarify what might otherwise be ambiguous requirements. The examples in the proposal are helpful, and would be especially appropriate for best practices. However, for guidelines, additional elaboration will be necessary for what is meant by "obtained unauthorized access to" and "not properly disposed of." Since this an extremely

[6] Such a step would be similar to steps taken by the agencies to help the industry address concerns over Y2K in 1999.

dynamic area, guidelines will also require the agencies to ensure examples are kept up to date. This is another reason the ICBA believes that the best practices approach is preferable.

CONCLUSION

The ICBA agrees that it is important for banks to take the appropriate steps to safeguard customer information. Community banks have been and will continue to be strong guardians of the security and confidentiality of their customer financial information. Community banks recognize that consumers are concerned about the security of their personal financial information, especially as technology revolutionizes data collection and retention and as the incidence of identity theft increases. Accordingly, as a matter of good business practice and as required by the Gramm-Leach-Bliley Act, banks have implemented and upgraded security measures to ensure customer information is properly secured.

The ICBA agrees that efforts must be made to detect and deter identity theft, and the individual customers should be made aware of situations where the security of their personal information has been breached. However, instead of the proposed prescriptive guidelines, the ICBA strongly urges the agencies to offer best practices that allow individual banks the flexibility and discretion to handle unauthorized access to customer information as appropriate.

Thank you for the opportunity to comment. If you have any questions or need any additional information, please contact ICBA's regulatory counsel, Robert Rowe, at 202-659-8111 or by e-mail at robert.rowe@icba.org.

Sincerely,

C. R. Cloutier

C. R. Cloutier
Chairman